eJournal of Tax Research (2022) vol. 19, no. 2, pp. 213-231

Identity theft tax refund fraud in the United States

Andrew Hultgren,[*] John Hasseldine[**] and Jonathan Nash[***]

Abstract

This article documents the phenomenon of identity theft tax refund fraud in the United States and describes the problem; including what it is, how the fraud is executed, its detection, magnitude and prevalence, and the response of key stakeholders. With a paucity of prior scholarly research and scant information from other countries, we rely on historical reports from the Internal Revenue Service (IRS) and its oversight agencies including the Government Accountability Office, Treasury Inspector General for Tax Administration, and the National Taxpayer Advocate. While metrics reflecting individual identity theft tax refund fraud have recently been trending in the right direction, the issue will have lasting consequences in terms of IRS resourcing and cybersecurity, taxpayer trust, tax preparation methods available to taxpayers and their compliance burdens – particularly the burden affecting low-income taxpayers, and on future tax compliance itself. Finally, this article is a call for scholarly attention both in the US and elsewhere, where the issue of this fraud has been under-researched.

Key words: cybersecurity; identity theft; IRS; tax administration; tax compliance; tax fraud

[*] FSO Tax Staff 1, Ernst & Young, Boston, USA. Email: andrewhultgren@gmail.com.
[**] Professor of Accounting and Taxation, Paul College of Business and Economics, University of New Hampshire. Email: john.hasseldine@unh.edu (corresponding author).
[***] Assistant Professor of Accounting, Paul College of Business and Economics, University of New Hampshire. Email: jonathan.nash@unh.edu. The authors wish to thank the Editors and two anonymous reviewers for their very helpful and detailed comments on an earlier version of this article.

1. INTRODUCTION

Identity theft (IDT) tax refund fraud in the United States has been a problem for the Internal Revenue Service (IRS) over the last 30 years, as well as at a state level. The first recorded instance of this type of fraud in the US occurred in 1988 as the *Los Angeles Times* reported that Donald Penrod had been indicted with the first ever charge of fraudulently filing tax forms electronically to receive an illegitimate refund (Nigrini & Peters, 2018, p. 39). By 1992 the Government Accountability Office (GAO; at that time, the General Accounting Office) identified the filing of fraudulent returns electronically as a major issue to be monitored and throughout the 2000s the problem continued to increase (GAO, 1992).

Although this article only focuses on the US, the problem clearly affects many countries. An Organisation for Economic Co-operation and Development (OECD) (2006) report on a survey to 19 members (i.e., countries) of a sub-group on Tax Crimes and Money Laundering examined the risks associated with IDT, how countries detected suspected cases, 'red flag indicators' of fraud, and the measures undertaken and results of these activities. Brief country case studies are reported on detection strategies and techniques, the use of multi-agency cooperation, and generic examples are provided of measures used such as data mining, data matching, risk profiling, inter-agency cooperation, training and public education.

This type of fraud allows fraudsters to maintain a degree of anonymity, complicating the successful prosecution of perpetrators. The growth of IDT tax refund fraud occurred as in the Information (Digital) Age, personal identifiable information (PII) was easier to obtain and the massive growth in federal and state tax return e-filing allowed this fraud to be perpetrated on a large scale. Federal tax e-filing has drastically increased throughout the 21st century. Only 58% of returns were filed electronically in 2008, but this escalated to 81% in 2012 and to over 90% by 2016 (Brody, Haynes & Mejia, 2014; Brink & Hansen, 2020).

The IRS first publicly recognised the problem when they issued their 'Dirty Dozen' list of tax scams in 2011, when they grouped tax refund fraud in with phishing,[1] but IRS then escalated their evaluation of the problem subsequently in 2012 – when identity theft topped the list (Meyerowitz, 2011; US Department of the Treasury, 2012). At this time, IDT tax refund fraud had already increased, so arguably the IRS was somewhat late in their assessment of the issue at hand, although the IRS had taken some actions to prevent it before the 'Dirty Dozen' list was released.[2]

The remainder of this article is structured as follows. The next section describes how IDT tax refund fraud is executed. Section 3 documents the development of this fraud and how the IRS has addressed the issue over three primary time periods. Section 4 outlines the responses by key oversight stakeholders to IRS actions based on reports published by GAO, the National Taxpayer Advocate (NTA), and the Treasury Inspector

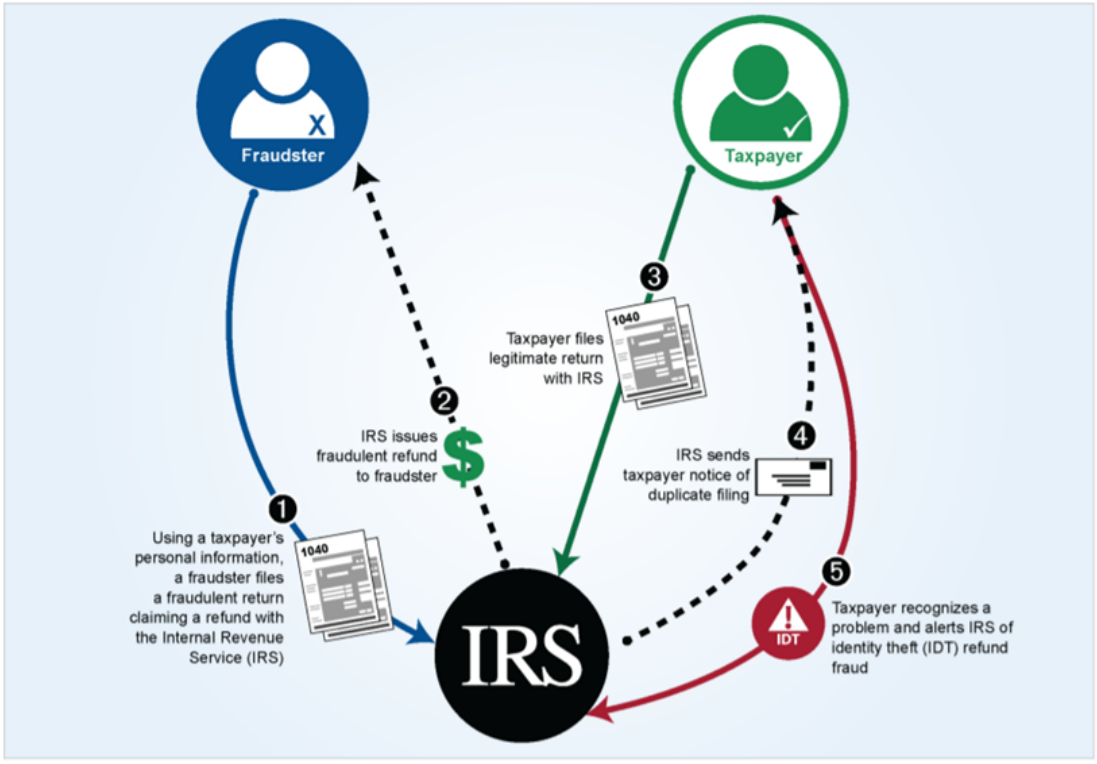
[1] Phishing occurs when a fraudster contacts a potential victim through a medium such as email or telephone and poses as a legitimate enterprise such as the IRS. The email/caller will then direct the victim to a website that appears legitimate and then the victim enters in their personal information for some stated purpose, such as it being required for their refund to be processed or to avoid a fee (Chambers & Zeidan, 2013).
[2] The 'Dirty Dozen' is an annual compilation published by the IRS of common scams that taxpayers may encounter throughout the year, although many of these schemes tend to peak during tax return filing season. See https://www.irs.gov/newsroom/dirty-dozen.

General for Tax Administration (TIGTA) and various outcomes including the *Taxpayer First Act 2019*. Section 5 then discusses several ancillary practical and scholarly implications at both individual and systemic levels before section 6 offers concluding remarks.

2. EXECUTION OF IDT TAX FRAUD

There are multiple methods to use IDT to commit tax evasion (OECD, 2006) but this section details the actual execution of tax refund fraud in the US. It is relatively straightforward and comprises three main steps starting with a fraudster obtaining a victim's PII, such as their name and social security number at a bare minimum, and then using this information to file a fraudulent tax return that provides them with a tax refund which is mailed to an address, or more often directly deposited to a bank account or prepaid debit card. When the legitimate taxpayer consequently files their return, it will be denied and the victim is forced into undertaking a lengthy remedial process (Thorne & Stryker, 2015). The process is shown graphically in Figure 1 (GAO, 2016, p. 8).

Fig. 1: Sample process for IDT tax refund fraud, United States



Source: GAO (2016, p. 8).

For the fraudster, obtaining the victim's PII is the initial barrier to perpetrating IDT tax refund fraud. Unfortunately, this is relatively easy in the modern era as fraudsters use a variety of tactics to obtain such information, one rampant method being through phishing through unsolicited emails and telephone calls. One sub-category of phishing schemes saw fraudsters posing as a senior company executive ostensibly emailing their own payroll or human resources department, requesting employees' PII and their wage and tax statement information from the employees' Form W-2 statements (GAO, 2018).

A further method has seen dishonest employees stealing PII from in-house databases through their employment and then either using the information to file fraudulent returns themselves or on-selling the PII to fraudsters. Other recorded instances include employees in prisons, educational institutions, medical facilities, and even within the IRS itself illegally downloading vast amounts of PII from databases for the purpose of committing IDT tax refund fraud (Nigrini & Peters, 2018).

Even the PII of deceased individuals can be used to commit this fraud. Historically, such information was easily available as it was published in newspaper obituaries. This then evolved in the modern era with firms providing individuals with hereditary data, such as Ancestry.com and Genealogy.com, even reporting the social security numbers of deceased individuals, although this practice stopped following pressure from the IRS (Fisk & Stigile, 2012).

Another major technique employed by fraudsters is the 'old-fashioned' technique of obtaining/stealing physical documents/equipment with PII on it. Fraudsters may 'dumpster dive' and sift through the trash of individuals looking for discarded tax returns, bank records, credit card receipts or other records containing PII or even search discarded laptop computers that contain information which can be used to perpetrate fraud (Chambers & Zeidan, 2013). They may obtain such data through home robbery where they steal documents with PII, or via pickpocketing a person's wallet, purse, or smartphone. Fraudsters may even steal a victim's mail either straight from their mailbox or more diabolically by submitting a change of address form to divert mail to an ulterior location (Fisk & Stigile, 2012).

Lastly, a method that is becoming more and more pressing is the purchase of PII from mass data breaches and hacking attempts (Nigrini & Peters, 2018). This enables organised groups to commit IDT fraud on a large scale and the quantity of information exposed by data breach is also increasing at an alarming rate.[3] Large scale data breaches are common, with the Equifax data breach in 2017 compromising varying amounts of PII for 143 million American consumers, or 44% of the US population, further arming fraudsters for all types of IDT fraud (Marcus, 2018).

The second step of creating the fraudulent return is a relatively straightforward process. Unfortunately, the IRS does not release detailed information on what schedules are used or what kinds of numbers fraudsters use for the withholdings and credits as this would essentially create a series of step-by-step instructions on how to commit the fraud. It is relatively simple to compile a return where the taxes due are less than the payments and credits, therefore generating a refund for the fraudster (Nigrini & Peters, 2018). Nowadays the more complex aspect of the fraud is creating a fraudulent return that is convincing enough to bypass the IRS's filters (discussed further in section 3). The filters

[3] Current data is publicly available from the Identity Theft Resource Center at www.idtheftcenter.org.

have gradually become more advanced throughout the years, thus necessitating fraudsters to continually evolve and hone their craft, creating gradually more convincing returns every year (IRS, 2018). NTA (2017a) noted an example of a more sophisticated scheme where criminals use employer identification numbers to file fraudulent business tax returns and concluded that the IRS must continue to remain vigilant and be nimble to counteract emerging developments in IDT fraud.

The third step in the fraud is to obtain the tax refund from the IRS. Most fraudsters use prepaid debit cards or direct deposits, with a slight tendency towards prepaid debit cards as these can be anonymously deposited without any direct tie to the fraudster (Chambers & Zeidan, 2013). Early on, a flaw allowed multiple tax returns to be filed from the same address, and according to TIGTA (2012) over 2,000 returns were filed from an address in Lansing, Michigan as well as hundreds of returns being filed from other specific addresses. Thankfully, this issue, as well as the issue of multiple refunds being deposited to one anonymous bank account, were alleviated following IRS action. Tax refunds must now be made to a bank account or debit card in the taxpayer's name and the number of refunds permitted to be sent to a single source is limited to three, but this has obviously been insufficient to completely prevent this final step of the fraud.

3. IRS ACTION ON IDT TAX FRAUD OVER TIME

3.1 Years prior to 2010

Despite some scrutiny from IRS oversight bodies (Hasseldine, 2015), the IRS was slow to publicly treat IDT tax refund fraud as a major issue and did not include it in their 'Dirty Dozen' list of scams until 2012. Notwithstanding this, over the years, the IRS has developed their techniques, administrative bodies, and procedural systems for dealing with the fraud.

In 2005, the IRS officially established the Identity Theft Program Office, later creating the Privacy, Information Protection, and Data Security office and the Identity Theft and Incident Management office with an accompanying Advisory Committee in 2007 (NTA, 2007). In 2008, the IRS began marking taxpayers' accounts within their database if taxpayers had been victims of this fraud, therefore helping to coordinate their efforts to assist taxpayers across various divisions. They also established the Identity Protection Specialized Unit to help taxpayers who had been victims as well as a toll-free hotline for victims to receive advice on the process that they would need to complete (NTA, 2008).

Beginning in 2009 the IRS implemented a series of filters or 'business rules' that could automatically assess if a return seemed fraudulent and flag it for screening by an actual IRS employee. The IRS also created an Identity Theft Affidavit in April 2009 (Form 14039), still currently used, so that taxpayers who knew they were victims of IDT tax refund fraud could notify the IRS of the issue, thereby streamlining the process somewhat for identity confirmation. Then also in 2009, the IRS initiated their educational campaign against falling victim to identity theft. By educating taxpayers and tax practitioners on methods to prevent becoming a victim of identity theft, the goal was to reduce fraud, and the IRS participated in over 40 events throughout the year, six of those being Nationwide Tax Forums (NTA, 2009).

3.2 Years 2010 – 2014

The IRS increased their efforts against IDT tax refund fraud in the years through 2014. In 2010 they implemented the Electronic Fraud Detection System, still in place to some extent to this day. The system was a more developed form of the filters that were used previously, as it would analyse returns both based on a series of general filters and based on prior year returns. It 'scores' tax returns and determines a probability of them being fraudulent, with those scoring above a certain (undisclosed) percentage being subject to further screening and extremely high scores being treated as fraudulent automatically (TIGTA, 2010).

In 2011, IRS created the Enhanced Return Processing program which sought to coordinate efforts throughout the various IRS divisions as NTA (2011) noted that 28 different subunits were involved in activities regarding identity theft. Part of this program was an initiative that sought to quell the number of fraudulent returns being filed with deceased individuals' information. This was accomplished in part by joint work with the Social Security Administration to begin marking the IRS accounts of deceased individuals and by putting pressure on websites such as Ancestry.com to cease listing the PII of decedents (Fisk & Stigile, 2012).

As 2012 was the first year that the IRS listed IDT tax refund fraud on its 'Dirty Dozen' tax scams, it is unsurprising that this year saw several advances made in the fight against fraudsters. For example, IRS assigned resources of 3,000 employees dedicated to the issue, with over USD 300 million spent (Nigrini & Peters, 2018). One of the most substantial programs introduced in 2012 was the Identity Protection Personal Identification Number program (NTA, 2012). This involves assigning taxpayers a specific number that they must use in order to file their return electronically (the medium that the fraud takes place in for the most part). The only taxpayers who were outright assigned a number were prior fraud victims, but additionally it was offered to taxpayers in Florida, Georgia, and the District of Columbia to opt into, as these were the areas that the IRS assessed as having higher fraud rates per capita (Hammel & Murolo, 2016).

A total of 251,500 numbers were issued in 2012 and 12,936 taxpayers then filed using an incorrect number, but this was later established to largely be due to human error and not a problem with the system (GAO, 2012). NTA (2012) did note that the numbers were all issued in one batch annually instead of issuing a number with every individual case that was brought to the IRS throughout the year.

Moreover, the IRS continued in its efforts to educate taxpayers through a digital approach, publishing up-to-date information on IDT tax refund fraud on their website and creating a series of YouTube videos and podcasts (Fisk & Stigile, 2012). They also decentralised their efforts by creating 21 specialised subunits to address the issue, but this approach was only partly successful (NTA, 2012).

Additionally in 2012, the Taxpayer Protection Program was created to analyse the returns identified by filters, which would also work with legitimate taxpayers who were falsely screened (TIGTA, 2018). Finally, the IRS created the Refund Fraud and Identity Theft Global Report which sought to consolidate and condense information about IDT tax refund fraud from various IRS divisions, and other governmental bodies, into one standalone report. This would then be used to further coordinate the IRS's efforts and serve as a management tool. This Global Report was significant as subunits were

previously compartmentalised, and the report was seen as an opportunity to create a more consistent strategic view (GAO, 2012).

Progress in 2013-2014 was slower. The IRS mandated that bank accounts be in the taxpayer's name to interfere with the second step of the fraudsters in acquiring the refund (TIGTA, 2012) and an online portal was created in 2014 for taxpayers to retrieve their PIN numbers, as previously taxpayers could only receive their PIN numbers and replacement numbers via mail (NTA, 2013). Congress also passed the *Stop Identity Theft Act* of 2014 which increased penalties for fraudsters and mandated the Department of Justice to collaborate with the IRS on future efforts, and to provide an annual report to Congress with updates (Thorne & Stryker, 2015). An Identity Theft Taxonomy was created to actually track and determine the amount of IDT tax refund fraud that was attempted, and the amount of refunds actually issued to false filers, as previously the IRS was relying mostly on estimates (GAO, 2014).

3.3 Years 2015 – 2020

During 2015, the IRS committed over 4,000 full-time employees and spent USD 470 million, but it was noted that even more funding would have proven useful (GAO, 2016). A revamp of the Electronic Fraud Detection System began with the testing of a new Return Review Process which had been in development since 2009 (GAO, 2015). The major benefit of this process was that in addition to the previous filters that relied on binary analysis, the new filters consisted of both rules and models. Additionally, the system was more flexible and its efficacy was seen in the first year as its false detection rate (the percent of legitimate returns flagged as fraudulent) was only 37.9% in comparison to a prior rate of 54.5% (NTA, 2016).

In 2015 the IRS also consolidated their IDT victim assistance functions into their Wage and Investment division, doing away with the 21 specialised units established in 2012 (NTA, 2014). A major benefit allowed victims to channel all their communications with the IRS through a single point of contact, rather than having to deal with numerous employees across different departments. There were still some cases requiring special attention, but most standard cases were now streamlined – previously advocated for many prior years (NTA, 2016). It was also reported in 2015 that the IRS increased the number of taxpayer accounts that had been marked as deceased to 28.4 million (TIGTA, 2015).

The most profound development from 2015 was the creation of the 'Security Summit', a meeting between 'IRS officials, the chief executive officers (CEOs) of the leading tax preparation firms, software developers, payroll and tax financial product processors, and state tax administrators' to discuss ways they could collectively address IDT tax refund fraud (IRS, 2015). The outcome of the Summit was a public-private partnership and the establishment of three work groups, based around authentication methods, information sharing techniques, and a Strategic Threat Assessment and Response working group designed to anticipate future issues. From the work groups came various ideas and initiatives such as improving the data elements in the filters and furthering external identity proofing procedures. They also worked on developing links with financial institutions, software companies, prepaid card companies and other third parties to share information with the IRS about developing trends in identity theft (IRS, 2015). Finally, the Summit discussed creating the framework for an Information Sharing and Analysis Center and a Cybersecurity Framework (first proposed in 2014) to further contest fraud (IRS, 2015).

In 2016 the Security Summit established additional work groups. Several programs were aimed at educating taxpayers and tax preparers, gaining nationwide media coverage (IRS, 2018). Separately, a collaboration with tax software providers helped to create more uniform secure standards for password creation and security questions. Finally, the Authentication Work Group introduced a pilot program to add a 16-digit verification code to 2 million Form W-2s (Wage and Tax Statements) in order to confirm that the submitted Form W-2s were legitimate accurate forms (Murolo, 2016). This helped to prevent fraudsters from concocting fictitious W-2s as it created an additional verification step, thus forcing fraudsters to steal accurate W-2s to acquire the code, therein making the fraud more complicated.

In 2017 another advance related to Form W-2 occurred with the acceleration of the W-2 submission deadline for employers to 31 January, previously 28 February in paper form (and 2 April electronically). Although this shift had been suggested as early as 2011 and had been reiterated for several years, it required Congressional approval in 2016 for its implementation (GAO, 2011; 2016). A late deadline in the tax filing season was problematic as it meant that the IRS could not match W-2 information to tax returns in real time, shown by the fact that the IRS had already issued nearly 60% of all tax refunds before they received a single W-2. This problem was further exacerbated by the fact that fraudsters would typically file very early on during the tax season in an attempt to file before the legitimate taxpayer. Moving the deadline forward proved to be effective as there was a 30% increase in received W-2 forms by March of 2017 (NTA, 2017b).

Other measures implemented in 2017 included the creation of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC) to allow the IRS, states, and industry partners to efficiently share information about developments in IDT tax refund fraud through an online platform and the creation of a collaborative organisation (GAO, 2017). When it was created, a total of 31 states, 14 tax preparation firms, and three financial institutions partnered with the IRS and the online platform was launched in January 2017. Since its inception, the partnership has grown drastically with 73 organisations currently participating and every state has joined to some extent (ISAC, 2018; 2020). Through their online portal, various entities can submit lead reports (‘leads’) of cyberthreats for the IRS to analyse. In just the first year of its inception, the IRS received over 1.8 million leads, but there was some trepidation from industry representatives who were unsure about the usefulness of their leads due to a lack of communication back from the IRS. The necessary feedback on the leads is however hampered by a lack of resources at the IRS and by rules which limit their ability to share taxpayer or record-level data (GAO, 2017).

In March 2017 a Rapid Response Team was deployed within the IRS to respond to events that created a significant threat of IDT refund fraud within 24-72 hours. The team would assess the situation and attempt to provide as much damage control as possible, and then around 2-3 days after the event, they would provide action steps for future prevention and methods for alleviation of the threat. The first threat responded to was the hacking of the IRS’s Data Retrieval Tool, which is a part of FAFSA.gov – a website for individuals to enter financial information to acquire need-based financial aid from the government. It was estimated that around 100,000 individuals had their PII stolen, but with the team’s actions, the IRS was able to prevent the issuance of over 8,000 fraudulent refunds and implement new security measures associated with the Data Retrieval Tool (GAO, 2017).

4. RESPONSE FROM OVERSIGHT AGENCIES AND OTHER OUTCOMES

4.1 IRS oversight agencies

As noted in section 3.2, GAO (2012) published an audit on electronic filing fraud when the US tax system was first starting to experience major problems and the amount of refund fraud was in the millions rather than billions (Nigrini & Peters, 2018). Additionally, NTA (2005) featured this method of fraud as one of their 'most serious problems' and noted that there was an additional TIGTA report on identity theft that asserted the IRS had no concrete corporate strategy in place to address the growing concern of the fraud.

The NTA and TIGTA both addressed the problem again in 2007 and found that there had been a 396% increase in the total number of complaints directed to the Federal Trade Commission, which was the only available indicator of the problem, given that the IRS had not yet begun closely monitoring IDT fraud at the time (NTA, 2007; TIGTA, 2007). The problem then worsened with GAO (2011) noting that the total number of incidents of tax-related IDT nearly quintupled from 2008-2010 growing from 51,702 to 248,357 cases. Overall, since 2005 the problem worsened, given it was consistently listed as one of the NTA's 'most serious problems' (although not in 2006, 2010, or 2014), leading to increased IRS action.

Early on, the NTA critiqued the IRS as taking an overall reactive stance to IDT tax refund fraud, with the NTA advocating for a more proactive approach (NTA, 2007). Generally, the IRS has sought to prevent individuals/organised groups from being able to commit refund fraud, rather than prosecuting specific fraudsters as they assessed this as being a more effective approach (Nigrini & Peters, 2018). Nevertheless, the Criminal Investigation branch did manage to convict approximately 2,000 identity thieves over the years 2013-2015 (IRS, 2016).

In addition, the GAO noted issues with the IRS's fraud estimates as their systems for quantifying the amount of fraud did not account for returns that passed underneath a certain (undisclosed) threshold, and there was also evidence of 'double counting' fraud cases under different systems, leading to the GAO (2016) recommendation of using return-level data to estimate the amount of fraud to provide Congress and other decision-makers with more accurate information.

One important consequence of IRS actions is the assertion that it has placed an undue, over-reaching compliance burden on everyday taxpayers through their efforts to combat fraud. GAO (2018, p. 6) shows just how difficult the challenge is for the IRS:

> Designing authentication programs involves a balancing act—IRS needs to prevent fraudsters from passing authentication using stolen taxpayer information, but it must balance that against the burden on legitimate taxpayers who must also authenticate. If IRS makes the authentication process too stringent, legitimate taxpayers may not be able to successfully authenticate to, for example, access their prior year tax information or have IRS release a frozen refund. Conversely, if the process is too easy, fraudsters will likely be able to authenticate as easily as legitimate taxpayers.

Notably, one way that the IRS has overburdened taxpayers is in the false detection rate of the Taxpayer Protection Program's filters (NTA 'Objectives Report', 2018). This is the rate at which legitimate tax returns are flagged as fraudulent, thus forcing the

taxpayer to verify their identity with the IRS. There has been a marked increase in the false detection rate of the filters over the years, from 20% in 2014 to 63% in 2019, even though the number of cases of IDT tax refund fraud has fallen over the years (NTA, 2020). In 2017, 1.9 million taxpayers were forced to verify their identities with 1.17 million completing the verification (GAO, 2018). In 2016 over USD 9 billion in legitimate refunds were delayed for an average of approximately 36 days (NTA, 2016). While this delay may not seem significant, it may impose significant hardship on low-income taxpayers. Low-income taxpayers often rely on their tax refund, of which the average was around USD 2,800 in 2016 to pay for various expenses and such delays can have a major impact in their lives (Greene, 2013; GAO, 2014; NTA, 2016).

TIGTA (2018) reports that there were 114 filters in place in 2014 and this grew to 200 filters by 2018. A high false detection rate from these filters has both a monetary cost to the IRS as employees must then deal with the authentications of legitimate taxpayers, but it may also lead to a side effect of decreased employee morale. NTA (2016) reports that studies have shown that when false detection rates exceed 25:1 employees become more careless as they assume their actions will not actually uncover fraud, therein decreasing employee engagement.

The process by which taxpayers must authenticate their identity has also been shown to be overly burdensome. High risk taxpayers must verify their identity in-person at a Taxpayer Assistance Center, of which there are around 400, by providing a government issued ID (GAO, 2018). In some cases, the closest office may be hundreds of miles away, or the closest one may not have available appointments for over a month, so if the taxpayer is low-income, or does not have access to transport, or is working multiple jobs, this is a daunting task that imposes substantial harm (NTA, 2017b). Low risk taxpayers can verify their identity over the phone, and while this may not seem overly burdensome, in many instances it is. For the 2016 filing season, the phone line received around 4.4 million calls, but it had a level of service (LOS), which is the proportion of phone calls that are answered versus the taxpayer hanging up before an operator answers, of only 22.7% on average which was the worst performance for any high-volume line operated by the IRS (NTA, 2016).

Given the IRS simply does not have sufficient resources devoted to these phone lines for it to be an effective method of authentication, this leads to additional frustration for fraud victims who are then forced through this authentication process when they are already under significant stress dealing with a stolen identity. Apart from tax fraud, IDT victims most likely will also have to deal with other types of IDT fraud (including utility, phone, bank, and employment fraud), and these can be problematic to remedy. NTA (2013) notes that psychiatrists have stated that the symptoms of IDT victims are similar to those of individuals suffering from post-traumatic stress disorder and it is therefore cruel to put these taxpayers through such a burdensome authentication process during such a vulnerable time (NTA, 2013).

4.2 *Taxpayer First Act 2019*

Apart from Congressional requests to oversight agencies (e.g., the GAO), Congress has shown its willingness to enact oversight legislation via the *Taxpayer First Act*. This Act was introduced with effect from 1 July 2019 to broadly redesign the IRS, expand and strengthen taxpayer rights, and enhance the IRS's cybersecurity. The *Taxpayer First Act* included the following four specific measures to increase protections and further assist identity theft victims (TIGTA, 2020):

(1) The IRS must create a program in which taxpayers, concerned that they may be a victim of identity theft, can request an Identity Protection Personal Identification Number (IP PIN) to file a tax return (section 2005).

(2) The IRS must establish a single point of contact for taxpayers who are a victim of identity theft. The single point of contact shall track the taxpayer's case to completion and coordinate with other IRS employees to resolve the case as quickly as possible (section 2006).

(3) The IRS must notify taxpayers when the IRS determines or suspects unauthorised use of the identity of an individual (identity theft), including the unauthorised use of the identity of the individual to obtain employment (section 2007).

(4) The IRS must develop and implement publicly available guidelines for management of cases of stolen identity refund fraud. The IRS must consult with the National Taxpayer Advocate and implement the guidelines not later than one year after the date of enactment (section 2008).

4.3 Recent outcomes and future measures

This section presents recent data on IDT tax refund fraud and what actions the IRS might take moving forward to both combat the fraud and protect public revenue, while still serving taxpayers' needs.

4.3.1 Recent outcomes

Despite the fact that the precise amount of fraud is incredibly difficult to estimate, as a whole the IRS has been shown to be making progress towards abating the problem. Even more encouraging is that it appears that the amount and rate of successful fraud are on the decline. The IRS reports three key metrics on IDT tax refund fraud.[4] Between 2015 and 2019, the number of taxpayers reporting they were IDT victims fell by 80%. This is based on taxpayers who file Form 14039 identity theft affidavits. In 2019, the IRS received 137,000 affidavits from taxpayers compared to 677,000 in 2015. This was the fourth consecutive year the number of affidavits received declined – based on the receipt of 199,000 affidavits in 2018, 242,000 in 2017, and 401,000 in 2016.

In addition to Form 14039 affidavits, between 2015 and 2019, the number of confirmed IDT theft tax returns stopped by the IRS declined by 68%. For 2019, there were 443,000 confirmed identity theft tax returns compared to 1.4 million in 2015. Starting in 2019, the IRS now allows victims more time to respond to inquiries about the questionable return, but the side effect is that this slows down the verification process. Given there were 649,000 confirmed identity theft returns in 2018, 597,000 in 2017 and 883,000 in 2016 remarkable progress has been made.

The final metric to examine is the amount of potentially fraudulent tax refunds prevented by the IRS. Again, for the period between 2015 and 2019, the IRS protected USD 26 billion in fraudulent refunds by stopping confirmed identity theft returns. In 2019, the 443,000 confirmed fraudulent returns sought to obtain USD 1.9 billion in

[4] See Internal Revenue Service, *Security Summit*, http://www.irs.gov/newsroom/security-summit.

refunds. In comparison, the IRS protected USD 3.1 billion in 2018, USD 6 billion in 2017, USD 6.4 billion in 2016 and USD 8.7 billion in 2015 – a 78% decrease overall.

4.3.2 Future measures

Despite these recent successes and the positive trends over the period 2015-2019, more can be done. The IRS could improve its authentication services, but opening more offices or increasing its phone line staffing would both be costly options for the chronically underfunded agency (NTA, 2019). Online methods are the most cost-effective methods of authentication for the IRS, but these can only be used for low-risk cases where taxpayers must answer questions based on prior years' tax returns, or for high-risk individuals who have set up multi-factor authentication with an IRS database. This method authenticates the taxpayer by sending a code to a mobile phone, thus ensuring the taxpayer possesses the phone, but if it has not been set up beforehand the taxpayer cannot use this method as a fraudster could simply set up the system with their own phone number, therefore making it worthless (GAO, 2018).

The IRS could also work to improve its filters and systems to decrease false detection rates and therefore the number of individuals who need to authenticate, and who then suffer delays in receiving their tax refunds. One possibility might be to create a filter system that implements machine learning that relies on models instead of simple binary rules (NTA, 2018). It could also use predictive models to determine more accurately the number of filters necessary, and adjust the filters more regularly, as in 2016 one filter had a false detection rate of around 91% and thus could have been discarded before the end of the filing season if the IRS possessed real time analytics (NTA, 2016). The IRS could also partner with financial industry experts with a proven track record of creating such systems and with the collaboration offered by the Information Sharing and Analysis Center, NTA (2016) considered this to be a beneficial opportunity. In a hearing before the House Committee on Oversight and Government Reform in April 2018, the IRS Commissioner agreed to try and bring false detection rates down to at least 50% (NTA, 2018).

Consistent with the provisions of the *Taxpayer First Act 2019*, the IRS expanded the IP PIN program into an optional nationwide scheme from January 2021 (three years ahead of the Act's July 2024 deadline). The number of PINs issued has steadily grown, from around 250,000 in 2012 to roughly 3.5 million in 2017, but hitherto this was only for prior victims of IDT refund fraud and residents of Florida, Georgia, and the District of Columbia who opted-in (Thorne & Stryker, 2015; GAO, 2018). By requiring every taxpayer to file with an IP PIN, the IRS could see impressive results – as an estimated USD 193 of revenue was protected for every taxpayer who received an IP PIN in 2014. As the cost of issuing IP PINs is only USD 36 for a three-year period, NTA (2015) calculates that on average, every dollar spent on the program has a USD 5.36 return. The question of where the original funding could come from may already be answered. Currently if a company such as Equifax is to blame for a massive data-breach, it will offer victims credit monitoring services, so the IRS could therefore attempt to shift this financial burden to the private sector, at least partially, especially as the rate of large-scale data breaches is growing. The only issue with this program is that the IP PIN would therefore become another piece of PII that fraudsters could steal, although it would at least make the fraud more difficult. Such a theft already occurred in March 2016 when hackers were able to obtain over 100,000 IP PINs by exploiting the IP PIN retrieval tool, and thus the system is not without its own vulnerabilities (GAO, 2017).

The most effective, but also most controversial tactic of combating IDT tax refund fraud would be to delay the tax filing season or refund issuances. This would allow the IRS to fully match return data with Form W-2s and give taxpayers more time to respond if their identity had been stolen. Unfortunately, this would likely have a disastrous impact on low-income taxpayers who rely on their tax refunds to survive (Greene, 2013) and such a course of action seems extremely unlikely.

5. IMPLICATIONS OF IDENTITY THEFT TAX FRAUD

5.1 Individual prevention

Individuals can pre-emptively take action to ensure that they are not victims of IDT tax refund fraud. The most obvious tactic is for the taxpayer to submit their individual tax return early in the filing season. If an individual files their return before fraudsters can, then taxpayers can drastically reduce the chance that they will become victims of the fraud (Chambers & Zeidan, 2013). This is by far the most effective method but given human nature to procrastinate on filing one's own taxes, it may also prove to be a difficult tactic to achieve.

Obviously, individuals should protect their PII and be wary of phishing attempts. These can take many forms, ranging from a call saying someone won a sweepstake, to an email that is purportedly from the IRS demanding action to avoid a fine, to even more advanced methods of emails that are 'spoofed' to look like they come from an employee at a place of work. The IRS regularly posts new forms of phishing and what taxpayers should be on the lookout for.[5]

Physical forms of PII should also be protected, i.e., never carry around such documents if it can be avoided, shred documents before disposal, protect incoming mail etc., and electronic PII can be safeguarded by keeping anti-virus software up to date, installing firewalls on home networks, visiting secure websites, taking care in the disposal of old computers/phones, and using strong, unique passwords as a rule of thumb. Moreover, individuals should regularly scan their own credit reports and bank statements to check for suspicious activity. Finally, IDT protection services can be used to protect/monitor one's identity, e.g., *LifeLock*, *Experian*, and *IdentityForce*.

Unfortunately, identity thieves target low-income taxpayers with poor credit and this group is also evidenced as being the most vulnerable to attack, together with identity theft occurring within abusive relationships (Dranoff, 2014). The delay in issuing tax refunds, described in section 4, is thus likely to interfere with recipients of the Earned Income Tax Credit and the low-income portion of the Child Tax Credit – two of the largest anti-poverty programs in the US. Greene (2021, p. 124) concludes that this leaves low-income IDT victims in a financial crisis, within a 'confusing system with few remedies that actually help them, and a mind-boggling number of steps and outreaches necessary to begin to recover their financial health. It is usually too little, too late'.

5.2 Tax professionals and cyber breach

Individuals may employ additional measures to give themselves peace of mind. Often when external tax preparers are used, e.g., via a certified public accountant or a tax

[5] See www.irs.gov/identity-theft-central.

preparer firm, this other entity will assist with the authentication process should one's identity be stolen. Some firms may charge an additional fee or offer add-on insurance that can be purchased separately. While this will not prevent the fraud from occurring, it will at least mean that taxpayers do not have to deal with the fallout from the fraud by themselves. Individuals can also file Form 8821 Tax Information Authorization, which means that if a return is filed in the taxpayer's name, they will receive a notification. Again, this does not prevent fraud, but if a person contacts the IRS before a refund is issued on the phony return, this can vastly accelerate the receipt of the legitimate refund while simultaneously preventing a fraudulent one (Thorne & Stryker, 2015).

Because tax preparation firms may themselves be targeted by fraudsters, the IRS recommends that tax professionals take critical steps to not only protect their clients, but also themselves from identity theft. Tax professionals must implement and maintain a data security plan and comply with Federal Trade Commission regulations and report any data theft immediately to local IRS liaisons and states for which the firm prepares returns – with detailed information contained in IRS Publications 4557 (Safeguarding Taxpayer Data) and 5293 (Data Theft Resource Guide for Tax Professionals).

Cybersecurity of professional firms, tax agencies, and even countries may also affect the ability of tax agencies in their desire to establish digital platforms and make taxes digital for taxpayers (Brink & Hansen, 2020; Ngugi et al., 2021). Hatfield (2018) notes that the US faces serious cybersecurity problems and that the IRS is itself a cyberattack target with taxpayer account information and databases reflecting a 'treasure trove of information' for criminals. Relatedly, then National Taxpayer Advocate Nina Olson's (2018, p. 2) personal comment at her plenary session at the 13th International Conference on Tax Administration, reveals the enormity of this issue: 'Cybersecurity, in fact, may prove to be the most significant impediment to broad digital usage in the US tax system', leading to her conclusion that encouraging the use of digital platforms, is not as simple, nor as desirable, as it first appears.

5.3 Tax compliance effects

There are virtually no scholarly publications on the effects of IDT on tax compliance itself. However, there are a small number that study the effect on taxpayers who have been subject to identity theft. For example, Kaspar et al. (2017) examine taxpayer attitudes and how they are influenced by IRS audits and identity theft investigations. Surprisingly, they find that only about 35% of taxpayers who experienced an IRS investigation involving a potentially fraudulent refund claim by someone improperly using their identification managed to recall the incident and they conclude that further research is necessary on how the duration and effectiveness of IDT tax refund fraud investigations affect taxpayer attitudes and behaviour.

Farrar, Hausserman and Pinto (2020) report on an experimental study that finds that the positive association between IRS responsibility for preventing identity theft tax refund fraud and future tax compliance intentions is mediated by trust in the IRS. Specifically, they find that when a tax authority is not to blame for IDT higher responsiveness by the tax authority significantly influences compliance through trust, but this effect is not present if the tax authority is to blame for the identity theft in the first instance. It seems plausible that the results of Farrar et al. (2020) may be relevant to general cybersecurity lapses in tax agencies as well.

6. CONCLUDING REMARKS

This article highlights IDT tax refund fraud as comprising a significant ongoing problem in the US tax system. Using information from public reports, we describe the problem and the overall response from the IRS and oversight agencies over the last three decades. OECD (2006) notes that IDT is a nuanced issue for tax agencies and this article shows that tax agencies must evaluate many factors including, but not limited to, the resourcing of tax agencies, decisions on how to effectively respond to the threat of IDT and evaluating the consequential effects on taxpayer burden and tax compliance. Ultimately, the problem has the potential to affect strategies on the digitalisation of tax systems.

Within the US, IDT tax refund fraud has been a high priority, in terms of resources devoted to the problem, and it has remained high on the annual IRS 'Dirty Dozen' list of scams since 2013. While the IRS certainly has not eliminated the fraud in its entirety, it is trending downwards, although it is difficult to point to a single tactic employed by the IRS as the 'most effective'. In this regard NTA (2017a) does however suggest that the improvement of the filters and systems the IRS uses, notably the implementation of the Return Review Program and the fact that the Form W-2 deadline was moved forward, were the primary causal drivers of the decrease in IDT tax refund fraud.

In the future, IDT tax refund fraud is likely to remain a constant threat as fraudsters will not simply let the IRS 'win' and will instead adapt and evolve their techniques to circumvent IRS filters. The full magnitude of the problem is still unknown, and the IRS must balance the importance of protecting public revenue versus the creation of remedial processes for taxpayer victims that are overly burdensome.

A recent example of how fraudsters have shifted emphasis and evolved is provided by the growing rise and threat of business-related refund fraud. This occurs when an employer's business information is fraudulently obtained, e.g., using an Employer Identification Number to commit fraud, so the challenges posed by individual IDT are also relevant to business IDT. In fact, the problem may be even more challenging given the ease with which business information is available, and the complexity of the business tax reporting environment (GAO, 2020a). A specific example of fraudsters evolving their methods is with employment-related identity fraud, which occurs when fraudsters use a name or social security number other than their own to obtain employment (e.g., if they are not authorised to work in the US or are trying to avoid maintenance payments, etc.), or to fraudulently receive Covid pandemic-related payouts. Victims may then face federal and state enforcement actions based on the wages earned, but unreported, by fraudsters (GAO, 2020b).

With a small number of notable exceptions as have been cited above, there are few peer-reviewed publications on the topic. However, this article is a call to action, as there are multiple areas for scholars to investigate in relation to the potential consequences of IDT tax refund fraud – including the resourcing of tax administrations and how they should implement internal systems and programs to deal with the fraud, how tax agencies can safeguard the PII of taxpayers and employers from fraudsters under tax system digitalisation initiatives, addressing the disproportionate effects of IDT fraud on low-income taxpayer victims including the financial and administrative burden placed on this group, and investigating any consequential effects of the fraud on taxpayer attitudes and compliance.

Finally, our study is limited in scope in that we do not examine other tax agencies' responses to identity theft refund fraud or the extent of the issue in other jurisdictions (e.g., Tzani-Pepelasi et al., 2020; Leighton-Daly, 2019). We also do not examine in detail, the emerging areas of business-related and employment-related tax refund fraud and general issues of tax reform and cybersecurity (Hatfield, 2018; Alm et al., 2020). All of the challenges described herein, seem likely to significantly impact tax administrations and influence taxpayers' level of trust in their own tax agencies.

7. REFERENCES

Alm, J, Beebe, J, Kirsch, M S, Marian, O & Soled, J A 2020, 'New technologies and the evolution of tax compliance', *Virginia Tax Review*, vol. 39, no. 3, pp. 287-356.

Brink, W D & Hansen, V J 2020, 'The effect of tax authority-developed software on taxpayer compliance', *Accounting Horizons*, vol. 34, no. 1, pp. 1-18.

Brody, R G, Haynes, C M & Mejia, H 2014, 'Income tax return scams and identity theft', *Accounting and Finance Research*, vol. 3, no. 1, pp. 90-95.

Chambers, V & Zeidan, R 2013, 'Stopping tax identity theft: Practical advice for CPAs and clients', *Journal of Accountancy*, February, pp. 60-64.

Dranoff, S 2014, 'Identity theft: A low-income issue', *American Bar Association Dialogue*, vol. 17, no. 2, pp. 1-2.

Farrar J, Hausserman, C & Pinto, O 2020, 'Trust and compliance effects of taxpayer identity theft: A moderated mediation analysis', *The Journal of the American Taxation Association*, vol. 42, no. 1, pp. 57-77.

Fisk, S M & Stigile, C 2012, 'Will the real John Doe please stand up? Tax identity theft developments', *Journal of Tax Practice & Procedure*, vol. 14, no. 1, pp. 21-71.

General Accounting Office (GAO) 1992, *Tax administration: IRS can improve controls over Electronic Filing Fraud* (GAO-93-27), GAO, Washington, DC.

Government Accountability Office (GAO) 2011, *Taxes and identity theft: Status of IRS initiatives to help victimized taxpayers* (GAO-11-721T), GAO, Washington, DC.

Government Accountability Office (GAO) 2012, *Identity theft: Total extent of refund fraud using stolen identities is unknown* (GAO-13-132T), GAO, Washington, DC.

Government Accountability Office (GAO) 2014, *Identity theft: Additional actions could help IRS combat the large, evolving threat of refund fraud* (GAO-14-633), GAO, Washington, DC.

Government Accountability Office (GAO) 2015, *Identity theft and tax fraud: Enhanced authentication could combat refund fraud, but IRS lacks an estimate of costs, benefits and risks* (GAO-15-119), GAO, Washington, DC.

Government Accountability Office (GAO) 2016, *Identity theft and tax fraud: IRS needs to update its risk assessment for the taxpayer protection program* (GAO-16-508), GAO, Washington, DC.

Government Accountability Office (GAO) 2017, *Identity theft: Improved collaboration could increase success of IRS initiatives to prevent refund fraud* (GAO-18-20), GAO, Washington, DC.

Government Accountability Office (GAO) 2018, *IRS needs to strengthen taxpayer authentication efforts* (GAO-18-418), GAO, Washington, DC.

Government Accountability Office (GAO) 2020a, *Identity theft: IRS needs to better assess the risks of refund fraud on business-related returns* (GAO-20-174), GAO, Washington, DC.

Government Accountability Office (GAO) 2020b, *Employment-related identity fraud: Improved collaboration and other actions would help IRS and SSA address risks* (GAO-20-492), GAO, Washington, DC.

Greene, S S 2013, 'The broken safety net: A study of Earned Income Tax Credit recipients and a proposal for repair', *New York University Law Review*, vol. 88, no. 2, pp. 515-588.

Greene, S S 2021, 'Stealing (identity) from the poor', *Minnesota Law Review*, vol. 106, no. 1, pp. 59-124.

Hammel, S W & Murolo, S B 2016, 'IP PINs: Fraud protection places duties on preparers', *Journal of Accountancy*, May, pp. 64-65.

Hasseldine, J 2015, 'Oversight mechanisms and administrative responses to tax complexity in the United States', in Evans, C, Krever R & Mellor, P (eds) *Tax simplification*, Kluwer Law International, Alphen aan den Rijn, pp. 275-292.

Hatfield, M 2018, 'Cybersecurity and tax reform', *Indiana Law Journal*, vol. 93, no. 4, pp. 1161-1209.

Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC) 2018, *Annual report*, Internal Revenue Service, Washington, DC.

Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC) 2020, *Annual report*, Internal Revenue Service, Washington, DC.

Internal Revenue Service (IRS) 2015, *2015 Security Summit: Protecting taxpayers from identity theft tax refund fraud*, IRS, Washington, DC.

Internal Revenue Service (IRS) 2016, *IRS, states and tax industry combat identity theft and refund fraud on many fronts*, 1 January, IRS, Washington, DC.

Internal Revenue Service (IRS) 2018, *Key IRS identity theft indicators continue dramatic decline in 2017; security summit marks 2017 progress against identity theft*, 8 February, IRS, Washington, DC.

Internal Revenue Service (IRS) 2019, *IRS concludes 'Dirty Dozen' list of tax scams for 2019: Agency encourages taxpayers to remain vigilant year-round*, 20 March, IRS, Washington, DC.

Kasper, M, Beer, S, Kirchler, E & Erard, B 2017, 'Audits, identity theft investigations, and taxpayer attitudes: Evidence from a national survey', in *National taxpayer advocate 2017 annual report to Congress – Vol. 2* (Washington, DC), pp. 148-193.

Leighton-Daly, M 2019, 'Identity Theft and Tax Crime: Has technology made it easier to defraud the revenue?', *eJournal of Tax Research*, vol. 16, no. 3, pp. 578-593.

Marcus, D J 2018, 'The data breach dilemma: Proactive solutions for protecting consumers' personal information', *Duke Law Journal*, vol. 68, no. 3, pp. 555-593.

Meyerowitz, S A 2011, '"Dirty Dozen" tax scams of 2011', *LexisNexis Legal News, Financial Fraud Law* (13 April), https://www.lexisnexis.com/LegalNewsRoom/financial-fraud-law/b/blog/posts/dirty-dozen-tax-scams-of-2011 (accessed 27 January 2021).

Murolo, S B 2016, 'Security summit touts improvements in its first year', *Journal of Accountancy*, September, p. 78.

National Taxpayer Advocate (NTA) 2005, *Annual report to Congress: 2005*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2007, *Annual report to Congress: 2007*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2008, *Annual report to Congress: 2008*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2009, *Annual report to Congress: 2009*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2011, *Annual report to Congress: 2011*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2012, *Annual report to Congress: 2012*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2013, *Annual report to Congress: 2013*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2014, *Annual report to Congress: 2014*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2015, *Annual report to Congress: 2015*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2016, *Annual report to Congress: 2016*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2017a, *Annual report to Congress: 2017*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2017b, *Objectives report to Congress: Fiscal Year 2017*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2018, *Objectives report to Congress: Fiscal Year 2018*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2019, *Objectives report to Congress: Fiscal Year 2019*, Internal Revenue Service, Washington, DC.

National Taxpayer Advocate (NTA) 2020, *Annual report to Congress: 2020*, Internal Revenue Service, Washington, DC.

Ngugi, B K, Hung, K-T & Li, Y J 2021, 'Reducing tax identity theft by identifying vulnerability points in the electronic tax filing process', *Information and Computer Security*, advance online, 30 August.

Nigrini, M J & Peters, J S 2018, 'Identity Theft Tax Refund Fraud: An analysis of the fraud schemes using IRS investigation summaries', *Journal of Forensic and Investigative Accounting*, vol. 10, no. 1, pp. 38-55.

Olson, N 2018, 'Some observations on tax administration and the digital revolution', plenary address at the University of New South Wales 13th International Conference on Tax Administration, UNSW Business School, Sydney, 5 April. Available at: https://www.business.unsw.edu.au/About-Site/Schools-Site/Taxation-Business-Law-Site/Documents/ime-Olson-Some-Observations-on-Tax-Administration-and-the-Digital-Revolution-paper.pdf.

Organisation for Economic Co-operation and Development (OECD) 2006, *Report on identity fraud: Tax evasion and money laundering vulnerabilities*, OECD Centre for Tax Policy and Administration, Paris.

Thorne, B M & Stryker, J P 2015, 'The "Dirty Dozen" tax scams plus 1', *Academy of Business Disciplines*, vol. 7, no.1, pp. 1-22.

Treasury Inspector General for Tax Administration (TIGTA) 2007, *Filing your taxes: An ounce of prevention is worth a pound of cure*, TIGTA, Washington, DC.

Treasury Inspector General for Tax Administration (TIGTA) 2010, *Interim results of the 2010 filing season* (2010-41-047), TIGTA, Washington, DC.

Treasury Inspector General for Tax Administration (TIGTA) 2012, *There are billions of dollars in undetected tax refund fraud resulting from identity theft* (2012-42-080), TIGTA, Washington, DC.

Treasury Inspector General for Tax Administration (TIGTA) 2015, *Results of the 2015 filing season* (2015-40-080), TIGTA, Washington, DC.

Treasury Inspector General for Tax Administration (TIGTA) 2018, *The Taxpayer Protection Program includes processes and procedures that are generally effective in reducing taxpayer burden* (2019-40-004), TIGTA, Washington, DC.

Treasury Inspector General for Tax Administration (TIGTA) 2020, *Constantly evolving refund fraud patterns require continued refinement and development of detection initiatives* (2020-40-040), TIGTA, Washington, DC.

Tzani-Pepelasi, C, Gavrilovic Nilsson, M, Lester, D, Roumpini Pylarinou, N & Ioannou, M 2020, 'Profiling HMRC and IRS scammers by utilizing trolling videos: Offender characteristics', *Journal of Forensic and Investigative Accounting*, vol. 12, no. 1, pp. 163-178.

US Department of the Treasury 2012, *IRS releases the Dirty Dozen tax scams for 2012*, 16 February, Washington, DC.